

Claim Amendment Summary

Claims pending

- At time of the Action: Claims 1-48.
- After this Response: Claims 1-48.

Canceled or Withdrawn claims: none.

Amended claims: none.

New claims: none

Pending claims are listed as follows:

1. **(ORIGINAL)** In a paging operating system having physical memory for holding information and secondary storage comprising a page file for receiving information that is paged out from the physical memory, a computer-implemented method of protecting information comprising:

encrypting information using a key that is page-locked in the physical memory; and

paging out, to the page file, the encrypted information.

2. **(ORIGINAL)** The computer-implemented method of claim 1 further comprising prior to said encrypting, creating the key and page locking the key in the physical memory.

3. **(ORIGINAL)** The computer-implemented method of claim 2, wherein said creating the key comprises creating the key during system boot up.

1 4. **(ORIGINAL)** The computer-implemented method of claim 2,
2 wherein said creating the key comprises generating a random key with a random
3 key generator.

4
5 5. **(ORIGINAL)** The computer-implemented method of claim 4,
6 wherein said generating comprises using RSA RC4 as an encryption algorithm to
7 generate the key.

8
9 6. **(ORIGINAL)** The computer-implemented method of claim 1,
10 wherein said encrypting comprises:
11 calling an operating system kernel;
12 the kernel using the page-locked key to encrypt the information.

13
14 7. **(ORIGINAL)** The computer-implemented method of claim 6,
15 wherein said calling is performed by an application.

16
17 8. **(ORIGINAL)** The computer-implemented method of claim 6,
18 wherein said calling is performed by an operating system memory manager.

19
20 9. **(ORIGINAL)** One or more computer-readable media having
21 computer-readable instructions thereon which, when executed by a computer,
22 perform the computer-implemented method of claim 1.

23
24 10. **(ORIGINAL)** An operating system programmed with instructions
25 which, when implemented by the operating system, implement the method of
claim 1.

1
2 11. **(ORIGINAL)** In a paging operating system having main memory
3 for holding information and secondary storage comprising a page file for receiving
4 information that is paged out from the main memory, a computer-implemented
5 method of protecting information comprising:

6 page-locking a key in main memory;
7 restricting access to the page-locked key to only the operating system
8 kernel;
9 calling the operating system kernel to encrypt information;
10 accessing the page-locked key with the operating system kernel; and
11 using the operating system kernel to encrypt the information with the page-
12 locked key.

13
14 12. **(ORIGINAL)** The computer-implemented method of claim 11,
15 wherein said calling is performed by an operating system memory manager.

16
17 13. **(ORIGINAL)** The computer-implemented method of claim 11,
18 wherein said calling is performed by an application.

19
20 14. **(ORIGINAL)** The computer-implemented method of claim 11
21 further comprising prior to said calling:

22 designating at least one page in the main memory with a designation;
23 recognizing the designation and, responsive thereto, calling the operating
24 system kernel to encrypt the information.

1 15. **(ORIGINAL)** The computer-implemented method of claim 14,
2 wherein said recognizing is performed by the memory manager.

3
4 16. **(ORIGINAL)** The computer-implemented method of claim 11,
5 wherein said calling comprises specifying a memory location and a memory size
6 associated with the information to be encrypted.

7
8 17. **(ORIGINAL)** One or more computer-readable media having
9 computer-readable instructions thereon which, when executed by a computer,
10 perform the computer-implemented method of claim 11.

11
12 18. **(ORIGINAL)** An operating system programmed with instructions
13 which, when implemented by the operating system, implement the method of
14 claim 11.

15
16 19. **(ORIGINAL)** In a paging operating system having main memory
17 for holding information and secondary storage comprising a page file for receiving
18 information that is paged out from the main memory, a computer-implemented
19 method of handling encrypted information comprising:

20 accessing encrypted information in the page file; and
21 decrypting the encrypted information with a key that is page-locked in the
22 main memory.

23
24 20. **(ORIGINAL)** The computer-implemented method of claim 19
25 further comprising placing the decrypted information in a page of main memory.

1 21. **(ORIGINAL)** The computer-implemented method of claim 19
2 further comprising placing the decrypted information in a page-locked page of
3 main memory.

4
5 22. **(ORIGINAL)** The computer-implemented method of claim 19,
6 wherein the page-locked key is accessible only to the operating system kernel.

7
8 23. **(ORIGINAL)** One or more computer-readable media having
9 computer-readable instructions thereon which, when executed by a computer,
10 perform the computer-implemented method of claim 19.

11
12 24. **(ORIGINAL)** An operating system programmed with instructions
13 which, when implemented by the operating system, implement the method of
14 claim 19.

15
16 25. **(ORIGINAL)** In a paging operating system having main memory
17 for holding information and secondary storage comprising a page file for receiving
18 information that is paged out from the main memory, a computer-implemented
19 method of protecting information comprising:

20 allocating a non-pageable page of main memory;

21 generating a random key; and

22 storing the random key in the non-pageable page of main memory, the
23 random key being configured for use by the operating system to encrypt
24 information that might be paged out to the page file.
25

1 26. **(ORIGINAL)** The computer-implemented method of claim 25,
2 wherein said generating comprises using an RSA RC4 encryption algorithm.

3
4 27. **(ORIGINAL)** The computer-implemented method of claim 25,
5 wherein said allocating takes place during system boot.

6
7 28. **(ORIGINAL)** One or more computer-readable media having
8 computer-readable instructions thereon which, when executed by a computer,
9 perform the computer-implemented method of claim 25.

10
11 29. **(ORIGINAL)** An operating system programmed with instructions
12 which, when implemented by the operating system, implement the method of
13 claim 25.

14
15 30. **(PREVIOUSLY PRESENTED)** In an operating system having
16 main memory for holding information and secondary storage for receiving
17 information that is transferred out of main memory, a computer-implemented
18 method of protecting information comprising:

19 generating at least one non-pageable random key by using a random key
20 generation process;

21 encrypting at least one selected block of information in the main memory
22 with a software component that uses the at least one random key for encryption;

23 transferring the one encrypted block of information to the secondary
24 storage;

25 decrypting the one encrypted block of information with the software
component that uses the at least one random key for decryption; and

1 placing the decrypted block of information in the main memory.

2
3 31. **(ORIGINAL)** The computer-implemented method of claim 30,
4 wherein said generating is performed during system boot up.

5
6 32. **(ORIGINAL)** The computer-implemented method of claim 30
7 further comprising restricting access to the at least one random key to only the
8 software component.

9
10 33. **(ORIGINAL)** The computer-implemented method of claim 30,
11 wherein the software component comprises the operating system's kernel.

12
13 34. **(ORIGINAL)** The computer-implemented method of claim 30
14 further comprising:

15 storing the at least one random key in the main memory; and

16 locking the at least one random key in the main memory so that it does not
17 get transferred to the second storage.

18
19 35. **(ORIGINAL)** An operating system programmed with instructions
20 which, when implemented by the operating system, implement the method of
21 claim 30.

22
23 36. **(ORIGINAL)** A system for use in protecting pageable information
24 comprising:

25 a memory having pageable and non-pageable pages; and

1 at least one key stored in the memory in a non-pageable page, the key being
2 configured for use in encrypting pageable information.

3
4 37. **(ORIGINAL)** The system of claim 36 further comprising a software
5 component that is configured to access and use said one key to encrypt pageable
6 information.

7
8 38. **(ORIGINAL)** The system of claim 37, wherein the one key is
9 accessible only to the software component.

10
11 39. **(ORIGINAL)** The system of claim 37 further comprising at least
12 one application configured to call the software component to encrypt the pageable
13 information.

14
15 40. **(ORIGINAL)** The system of claim 37 further comprising a memory
16 manager configured to call the software component to encrypt the pageable
17 information.

18
19 41. **(ORIGINAL)** A computer program embodied on one or more
20 computer-readable media, the program comprising:

21 encrypting information with a key that is page-locked in main memory of a
22 computer;

23 paging out, to secondary storage, the encrypted information;

24 accessing the encrypted information in the secondary storage; and

25 decrypting the encrypted information with the key that is page-locked in the
main memory.

1
2 42. **(ORIGINAL)** A programmable computer comprising:
3 a processor;
4 main memory for holding information;
5 secondary storage for receiving information that is temporarily transferred
6 out of the main memory;
7 the computer being programmed with computer-readable instructions
8 which, when executed by the processor, cause the computer to:
9 encrypt information that is to be transferred to the secondary storage with a
10 key that is locked in the main memory;
11 transfer the encrypted information to the secondary storage; and
12 decrypt the encrypted information with a key that is locked in the main
13 memory.

14
15 43. **(ORIGINAL)** The programmable computer of claim 42, wherein
16 the instructions cause the computer to generate the key and lock the key in the
17 main memory.

18
19 44. **(ORIGINAL)** The programmable computer of claim 42, wherein
20 the key that is used to encrypt the information is the same key that is used to
21 decrypt the information.

22
23 45. **(ORIGINAL)** The programmable computer of claim 42, further
24 comprising a software component that is programmed to encrypt and decrypt the
25 information.

1 46. **(ORIGINAL)** The programmable computer of claim 45, wherein
2 the software component comprises the operating system's kernel.

3
4 47. **(ORIGINAL)** One or more application programming interfaces
5 embodied on one or more computer-readable media for execution on a computer
6 in conjunction with a paging operating system having main memory for holding
7 information and a page file for receiving information that is paged out from the
8 main memory, comprising:

9 an interface method for encrypting pageable information with a key that is
10 page-locked in the main memory; and

11 an interface method for decrypting encrypted information that is contained
12 in the page file.

13
14 48. **(ORIGINAL)** An application programming interface embodied on a
15 computer-readable medium for execution on a computer in conjunction with a
16 paging operating system having main memory for holding information and
17 secondary storage comprising a page file for receiving information that is paged
18 out from the main memory, comprising a method for setting an attribute on a page
19 of main memory, the attribute designating that the page must be encrypted with a
20 key that is page-locked in the main memory prior to the page being paged out to
21 the page file.